October 7, 2025

Prague

How is the European Commission planning to break cryptography this time?

Marcel Kolaja <marcel@accessnow.org>

Policy & Advocacy Director – Europe, Access Now

OpenSSL Conference 2025

accessnow

Access Now defends and extends **the digital rights of people and communities at risk.**

120+ staff

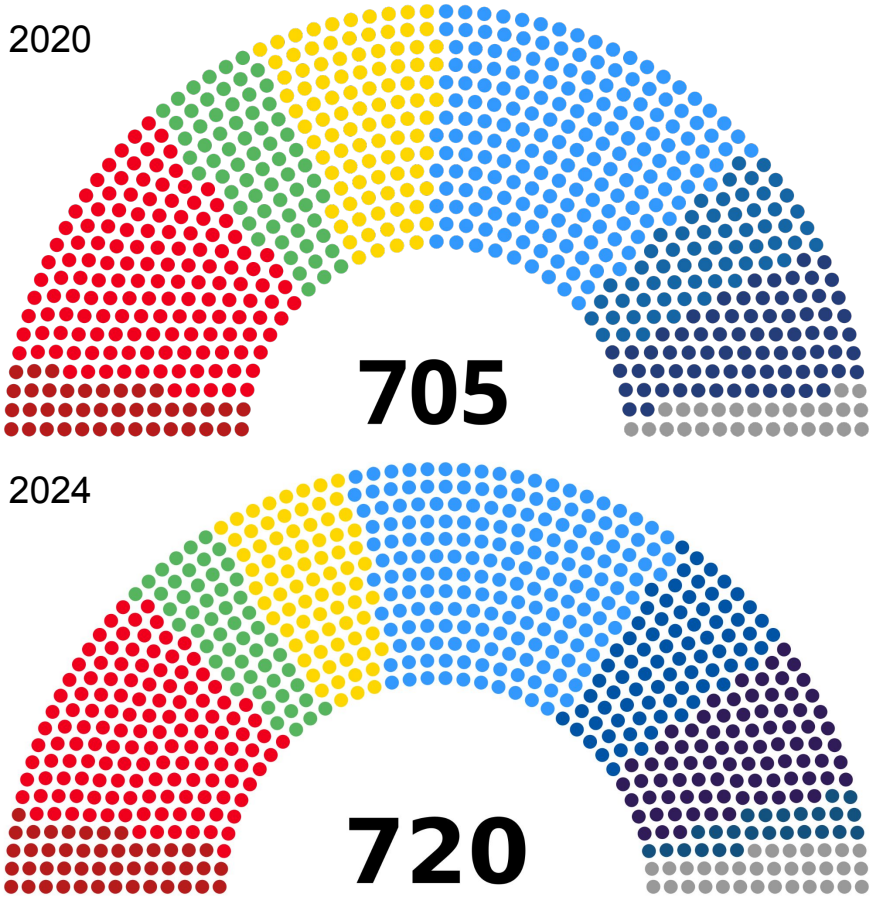
7 **global regions**
and officially registered in **4** countries

HLG on access to data

- In June 2023, the European Commission sets up a *High-Level Group on access to data for effective law enforcement.*
- The group is *tasked to explore any challenges that law enforcement in the Union face in their daily work in connection to access to data and explore and contribute to finding potential solutions to overcome them, with the aim of ensuring the availability of effective law enforcement tools to fight crime and enhance public security in the digital age*.
- In May 2024, the HLG adopts a set of recommendations, including *establishing a research group to assess the technical feasibility of built-in lawful access obligations (including for accessing encrypted data) for digital devices.*
- In June 2024, the Council of the European Union holds an exchange of views on the HLG's recommendations. One of the priorities that the home affairs ministers identified is *establishing legally and technically sound solutions for accessing encrypted electronic communication in individual cases and subject to a judicial order for the purpose of preventing, investigating and prosecuting serious and organised crime and terrorism*.

2024 European Elections

- 5 year term of the European Parliament: 2024–2029
- von der Leyen Commission II
- “Securitization” narrative strengthens the political appetite for lawful access to encrypted data, even though it removes security by definition.



ProtectEU

- European Internal Security Strategy
- Published by the European Commission on April 1, 2025, unfortunately, not as a joke.
- Replaces the European Security Union Strategy, which led to the Chat Control proposal among others.
- *Sets out the objectives and actions for the next years to ensure a safer and more secure Europe.*
- The Commission will present a Technology Roadmap on encryption to identify and assess technological solutions to enable lawful access to encrypted data by law enforcement authorities in 2026.
- The political narrative contrasts with the technical reality: the objective cannot be achieved without weakening encryption and security.

Potential impact

- Weakening encryption is detrimental to fundamental rights enshrined in the Charter of Fundamental Rights of the European Union
  - Protection of personal data (Article 8)
  - Freedom of expression and information (Article 11)
- There is no technical lawful access to end-to-end encrypted communication without breaking privacy and security.
- Client-side scanning breaks privacy and security.
- Risk of disproportionate surveillance and lack of judicial oversight
- Companies avoiding Europe or implementing weaker security leads to innovation slowdown.
- Research funding shift: access to encrypted data instead of strengthening security
- Potential danger for Free and Open Source Software

Let’s frame the debate correctly

- **Strong encryption is essential for security and protects national security:** Encryption is a mathematical process that cannot be selectively applied. Any demand for a backdoor that only works for the government is essentially at war with mathematics.
- **Giving law enforcement exceptional access threatens human rights and democracy:** Encryption is critical to democratic governance and the protection of the right to privacy and the right to freedom of expression in the digital age. Weakening encryption through exceptional access mechanisms jeopardizes these basic human rights, and democracy as a whole.
- **Strong encryption strengthens privacy *and* security:** The framing of the debate on encryption policy as “privacy versus security” is inaccurate and premised on a false binary. The two are mutually reinforcing principles. A more appropriate framing of the debate would be “security versus security,” as encryption not only protects privacy, it protects security.
- **Backdoors to encrypted systems will not stop criminals and terrorists from using strong encryption.**

What can be done

- Support civil society organizations, coalitions, and networks, e.g. Access Now, Center for Democracy & Technology, Internet Society, Article 19, Bits of Freedom, Electronic Frontier Foundation, Global Encryption Coalition, EDRi, and many more
  - Read newsletters
  - Follow social networks
- Advocacy efforts
- Talk to policymakers
- Participate in public consultations
- Raise public awareness

Questions?

accessnow